图书情报工作
第64卷 第5期 2020年3月

数据保护影响评估制度：欧盟立法与中国方案*

■ 崔聪聪 许智鑫
北京邮电大学互联网治理与法律研究中心 北京 100876

摘 要：［目的/意义］欧盟一般数据保护条例（GDPR）引入的数据保护影响评估（DPIA）制度给数据控制者提出新的要求。通过解析 GDPR 中 DPIA 制度的相关规定，研究其立法思路和核心理念，可以为我国相关立法工作提供借鉴。［方法/过程］通过查阅和梳理以 GDPR 为代表的欧盟数据保护领域的法律文件，归纳 DPIA 制度的出台背景和演化过程，深入剖析 DPIA 制度的数据保护模式、适用情形、基本流程和执行过程等主要内容。［结果/结论］DPIA 制度能够应对愈加复杂多变的数据安全风险环境，具有重要的实践价值和参考意义。我国个人信息保护法应确立 DPIA 制度，具体内容包括 DPIA 的规制对象、适用情形以及数据控制者的事先咨询义务，并提出数据风险评估模型。

关键词：数据保护影响评估 风险路径 数据风险评估模型 个人信息保护法
分类号：G250
DOI：10.13266/j.issn.0252-3116.2020.05.005

1 引言

伴随着云计算、大数据、物联网和人工智能等新技术和新应用的出现，对个人数据进行的自动化处理变得无处不在，个人的权利和自由在数字时代受到了前所未有的威胁。2012 年 1 月，欧洲委员会启动了欧盟个人数据保护立法的改革进程，提出制定《通用数据保护条例》（General Data Protection Regulation，GDPR）以取代已有的《关于个人数据处理保护与自由流动指令》（Directive 95/46/EC，以下简称《95 指令》）。GDPR 于 2018 年 5 月 25 日正式生效，其作用在于协调欧盟国家数据保护法律的一致性，保护并强化欧盟公民的数据权利，重塑组织机构数据处理的方式[1]。在众多具有创新性的制度中，GDPR 特别引入了数据保护影响评估制度（Data Protection Impact Assessment，DPIA）。

DPIA 制度是第一个被纳入欧盟数据保护法的风险管理工具，旨在描述数据处理行为，评估其必要性和适当性，并通过评估内容确定这些问题的应对措施，帮助管理个人数据处理活动对自然人带来的威胁和风险。此外，DPIA 是建立和展示数据处理活动合规性的方法，用于帮助数据控制者遵守 GDPR 的相关规定，证明其已采取适当措施以遵守欧盟数据保护法规[2]。DPIA 制度作为欧盟数据保护框架中的核心内容，受到国内外企业和监管机构的广泛关注，为各国应对日益增长的数据安全风险问题提供了理想的立法范本。

目前，欧盟学术界仅有 R. Gellert[3]、F. Bieker 等[4]少数几位学者对 DPIA 制度的理念和实践进行了初步分析，主要聚焦于从隐私影响评估制度（Privacy Impact Assessment，PIA）转变为 DPIA 制度过程中数据风险概念的改变，以及基于 GDPR 文本内容的企业合规方法，除此之外未有更为深入和系统性的研究成果。而国内的相关研究多停留在泛泛介绍 DPIA 制度，提倡对数据处理行为规制的思路转换，对国内相关法律法规提出较为有限的调整建议。至于我国个人信息保护立法应当如何借鉴 DPIA 制度，尚未有学者涉及。本文通过解析欧盟 GDPR 中数据保护影响评估制度的相关规定，研究 DPIA 制度的演化过程和核心理念，提出我国 DPIA 的制度设计，构建以风险管理为路径的数据保护体系，期冀为我国已经启动的个人信息保护立法提供参考。

* 本文系国家社会科学基金重大项目“国家网络空间安全法律保障机制研究”（项目编号：13&ZD181）研究成果之一。
作者简介：崔聪聪（ORCID：0000-0001-7633-1007），副主任，副教授，博士，E-mail：cuicongcong@bupt.edu.cn；许智鑫（ORCID：0000-0002-5149-5678），硕士研究生。
收稿日期：2019-05-06 修回日期：2019-10-09 本文起止页码：41-49 本文责任编辑：王传清

2 欧盟 DPIA 制度的背景和演化

2.1 GDPR 设立 DPIA 制度的背景

GDPR 第 35 条第 1 款规定了 DPIA 的一般要求：数据处理行为，特别是在运用新技术可能会给自然人的权利和自由带来高风险时，数据控制者应当在进行数据处理行为之前综合考虑该行为的性质、范围、背景和目的，评估预期行为可能给个人数据保护带来的影响[5]。在 GDPR 出台以前，欧盟已有对特定的技术应用进行数据保护影响评估的要求：一是针对 RFID 应用领域的隐私影响评估和数据保护影响评估框架（Data Protection Impact Assessment Framework，DPIAF）[6]；二是欧洲委员会智能电网工作组提出的针对智能电网和智能计量系统的 DPIA 模板[7]。这两份文件分别由欧盟 WP29 工作组评价和建议并进行了相应修订。欧盟在前期出台的数据保护评估文件的基本要点均参照了《95 指令》的相关内容，但实际执行影响评估的过程均因相关文件内容的不同而各有差异[8]。

相比于 PIA 和 DPIA，技术评估（technology assessments）和环境影响评估（environmental impact assessments）是影响评估领域的先行者[9]。GDPR 引入的数据保护影响评估制度是影响评估这一领域的新入者。一方面它没有直接照搬相关的影响评估制度；另一方面，它被认为与 PIA 有许多相似之处。后者从 20 世纪 90 年代开始逐渐发展，主要在盎格鲁－撒克逊国家普遍应用[10]。有关 PIA 的相关观点和文献，以及数据保护机构（Data Protection Authorities，DPAs）发布的指导文件[11]，都对欧盟 DPIA 制度的构建有潜在的影响。

2.2 从 PIA 到 DPIA

DPIA 制度建立在 PIA 制度基础之上，是对后者进行转用和继承的产物[12]。PIA 制度被定义为一种评估方法，用于分析判定个人信息处理项目、政策、计划、服务、产品或者其他活动对隐私产生的影响，并要求与利益相关方协商合作，采取必要的补救措施以避免或减少负面影响[13]。作为欧洲最早实施 PIA 制度的国家，英国于 2007 年由信息专员办公室（Information Commissioner's Office，ICO）发布 PIA 行为准则以细化和补充英国《数据保护法》第 51 条的相关规定，通过建立多环节的 PIA 标准执行流程，评估和降低在个人信息处理项目生命周期中的隐私风险；法国国家信息和信息自由委员会（Commission Nationale de l'Informatique et des Libertés，CNIL）于 2015 年出台了 PIA 保护框架，侧重于建立一套以技术手段和组织手段为核心的风险防控制度，以支持和保护数据主体的隐私权。

在欧盟范围内建立的 PIA 制度通常包括以下 5 个步骤：阈值分析（确定 PIA 是否必要）、数据处理行为说明、风险评估、风险管理以及最终报告，其完整执行流程是一项多学科、多领域的项目，需要利益相关者和公众的多方参与。PIA 制度作为 DPIA 制度的前身，具备许多与后者相类似的特征：首先，PIA 被认为是一个持续性的动态执行过程，需要在数据处理活动的生命周期中持续进行且不断更新；其次，各国都将 PIA 视为一种风险预防手段，提倡组织机构在项目部署的早期便开始进行，以便具有最大的杠杆作用；再次，PIA 可作为一种风险管理工具，用于系统性地评估隐私或数据保护的风险，并要求能够设计解决方案以减轻由评估得出的风险[14]。

PIA 制度的建立在欧盟范围内起到了一定的隐私保护规范作用，但由于出现在 DPIA 法律义务正式设立前，其始终未能成为强制性的法律义务，在很大程度上只能起到建议和引导作用。此外，包括英国和法国发布的 PIA 文件在内，欧盟各国设立的 PIA 制度普遍采用了清单式检查方法。尽管通过列举方式能够明晰地表明评估内容，降低组织机构进行 PIA 的执行难度，但会导致组织机构过度关注于已列明的固定风险，既无法适应风险环境的动态变化，也无法关注不同数据处理行为的特定风险和要求。

相较于在先的 PIA 制度，欧盟 GDPR 设立的 DPIA 制度能够协调各成员国间数据保护法律的一致性，不仅成为了欧盟统一数据保护法律框架下的强制性义务，同时具备较强的可扩展性和动态调整能力。但 DPIA 制度的规制范围仅限于数据保护领域，并非解决 PIA 制度所关注的隐私保护问题。总体而言，通过借鉴 PIA 制度的设立思路和实施经验，DPIA 制度具备更强的可操作性，既是一种合规工具也是一项法律义务，在保障数据处理活动持续安全的同时，确保数据控制者和处理者的数据处理活动合理合法。

3 欧盟 DPIA 制度的理论基础和主要内容

作为针对数据处理活动进行风险评估的制度，DPIA 制度的理论核心是“风险路径（risk-based approach）”，包括描述数据处理过程、识别和评估风险、减轻和应对风险等一系列的风险管理步骤。GDPR 在第 35 条系统规定了 DPIA 的各项要求，还在“控制者义务”“数据保护官”和“监管机构”等多个章节进一步细化了 DPIA 的相关要求。

3.1 以风险管理为路径的数据保护模式

3.1.1 数据保护中的风险构成

对风险的合理判定是正确建立 DPIA 制度的前提条件。对风险的分析通常表现为客观和中立的,但不尽然。有学者认为,任何与风险有关的决定都涉及两个截然不同但又不可分割的因素:客观事实和主观观点[15]。无论是对社会治理领域[16]还是科学技术领域[17]的风险研究均表明基于风险的实践总是与其所处的社会环境和社会价值密切相关。尽管如此,数据保护中的风险仍需要能够具体落地的方法论、模板和流程等统一的抽象概念[18]。

GDPR 规定的风险处理手段反映了风险的双重维度:风险评估和风险管理。风险评估衡量客观的风险水平,侧重于可能性和严重性的分析,其流程可分为风险标准、风险识别和风险评估步骤[19];风险管理的重点是决定是否承担风险,其决策通常附带旨在降低风险水平的措施[20]。

为了更好地绘制和理解 GDPR 中风险的概念,需要对风险本身的构成进行分析。欧盟 WP29 工作组将风险定义为"描述事件及其后果的预想,根据严重性和可能性进行预估"。具体而言,数据保护中的风险构成应当包含三要素:①事件,特定情况的发生或者变化。它可能发生也可能不会发生,并且会产生一些积极或消极的后果。②后果,事件的结果。当这种影响是负面时,它们可以被称为危害;当影响是积极时,它们可以被称为利益。③风险因素,单独的或者组合的要素具有引发危害的内在潜力。这些决定了风险是否发生以及如何发生,并确定风险的严重程度。

3.1.2 数据保护模式转向风险管理

在大数据时代,以"知情同意原则"为基本路径的个人信息保护法已逐渐流于形式,其不仅给用户和组织带来了沉重负担,而且未真正赋予用户实际的数据控制权[21]。因此,GDPR 引入的 DPIA 制度可被视为将数据保护的监管和立法路径从"知情同意"转向"风险路径"的重要举措。

欧盟 DPIA 制度将关注点由数据处理行为的统一监管转变为针对特定数据处理行为的动态风险管理,并贯穿于项目规划和执行过程中,以尽早地发现、评估、应对有关数据保护、个人权利和自由的显著风险[22]。由于数据处理行为的普遍性和瞬时性,信息传播往往具有广泛性和不可控性,风险危害发生后可能会给个人和组织机构带来难以挽回的损害,因此保护数据的最佳方案应聚焦于损害发生之前的防控措施而非事后的补救方法。欧盟 DPIA 制度重新建立并拓展了传统的数据保护模式,侧重于事前的预防方法,强调"风险分析""影响评估"和"生命周期管理"等理念的引入和运用,通过对数据保护风险的评估和管理,促使数据保护的传统监管模式转向以风险管理为路径的新型数据保护模式。

3.2 欧盟 DPIA 制度的基本内容

3.2.1 DPIA 制度的适用情形

GDPR 的适用范围包括在欧盟法管辖范围之内的所有完全自动化或者部分自动化个人数据处理行为,以及形成或者旨在形成数据画像的非自动化个人数据处理行为。尽管每个受到 GDPR 规制的相关组织都将存在数量可观的数据处理活动,但 DPIA 的强制性义务并非针对组织机构的每一项数据处理行为,否则在实践之中 DPIA 制度将不具有可操作性和经济性。总体而言,除非相关数据处理行为满足了 GDPR 规定的豁免条件,否则只要符合"可能会给自然人的权利和自由带来高风险"的数据处理行为均需要执行 DPIA 方法。

而当数据处理行为不具备高风险的可能性时,相关组织将不需要履行 DPIA 义务。除此之外,当数据处理行为的性质、范围、背景和目的与已有的 DPIA 非常相似时,可以使用已有的 DPIA 结果进行类似处理,而无需执行新的 DPIA 方法;或者当处理行为在法律中被特别授权,且该法律在设立之时已经执行了相应的 DPIA,则无需再执行 DPIA 方法;或者当数据处理行为符合主管部门规定的正面清单要求,则该处理行为无需执行 DPIA 方法,但仍需严格按照正面清单所要求的行为范围和相关条件开展处理活动。

除建立豁免 DPIA 义务的正面清单以外,GDPR 同时要求监管机构应当制定数据保护影响评估的负面清单,从而以清单式方法明确必须或者无需进行 DPIA 的数据处理行为。对于具有强制性义务的数据处理行为,GDPR 特别地要求当一项新的数据处理技术被引入时,相关组织应当主动进行数据保护影响评估。此外,当存在以下三种情形之一时,相关组织应当进行数据保护影响评估:①对自然人个人情况进行系统、广泛的评估,该评估以自动化决策系统和数据画像为基础,评估结果能够影响自然人的权利或者义务;②对特殊类型的个人数据或者与刑事定罪和犯罪行为相关数据的处理活动;③公共领域的大规模系统性监控活动。

从文本上来看,GDPR 所规定的 DPIA 具体适用情形较为模糊和有限,但同时为欧盟相关监管机构预留了一定的自由裁量权,实际工作中的 DPIA 义务适用范

围仍需要以法律文本为基础,结合具体业务实践确定。

3.2.2 DPIA 制度的基本流程

对于开展数据处理活动的组织机构而言,为实现在欧盟 GDPR 框架下的合规要求,避免因违反 DPIA 强制性义务而遭受巨额罚款和其他严重后果,其应在数据业务活动中主动执行 DPIA 的基本流程,主要包含 4 个步骤:①对是否可能造成高风险的判断;②对是否适用于例外情形的判断;③执行 DPIA 方法;④对剩余风险是否仍然高的判断。而后相关组织将根据实际的风险程度决定是否向监管机构进行事先咨询,如图 1 所示:

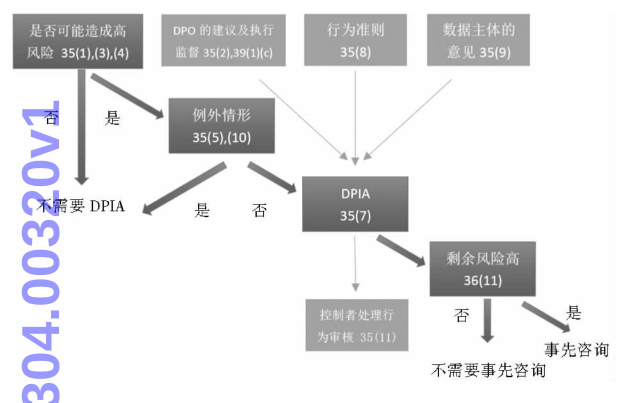


图 1 DPIA 制度的基本流程及其对应 GDPR 条文

(1)对是否可能造成高风险的判断。作为数据控制者的组织机构应当充分考虑数据处理行为的性质、范围、背景和目的,对数据处理行为可能对自然人权利和自由带来的高风险在事前进行评估。若相关组织认定风险程度确实较低,则不需要再继续执行 DPIA 制度的后续流程。

(2)对是否适用于例外情形的判断。数据控制者应当根据 GDPR 规定的豁免条件确定是否能够免于执行 DPIA:一种是监管机构根据 GDPR 第 35 条第 5 款,由监管机构列举的不需要进行 DPIA 的数据处理行为;另一种是根据 GDPR 第 35 条第 10 款规定的具有特定法律依据的数据处理行为。若相关组织判定其数据处理行为与已有的 DPIA 方法的风险情形非常相同,则可在该步骤中对适用方法予以确认。

(3)执行 DPIA 方法。在 DPIA 方法的执行过程中,数据控制者应当就进行数据保护影响评估的具体方法寻求数据保护官(data protection officer, DPO)的意见和帮助,并将欧盟成员国、行业协会等机构制定的行为准则考虑在内。在不妨害商业利益、公共利益以及处理行为安全性的前提下,数据控制者应当就数据处理行为向数据主体或者其代理人征求意见。数据控制者应当对相关数据处理行为进行监督,确保 DPIA 评估结果及风险应对方法的实施。

(4)对剩余风险是否仍然高的判断。如果 DPIA 评估结果表明相关组织没有采取足够的数据保护措施以减少数据处理行为过程中产生的高风险,则数据控制者应当在开始数据处理活动之前向监管机构进行事先咨询。如果监管机构认为数据控制者或者处理者将要开展的处理活动会违反 GDPR 的规定,尤其当数据控制者不能充分地识别或者降低风险,应在收到咨询请求的 8 周内(根据数据处理活动的复杂性,还可以再延长 6 周),向数据控制者和数据处理者提供书面建议。

3.2.3 DPIA 方法的具体实施

(1)执行主体。DPIA 方法的执行是基本流程的第 3 步,也是 DPIA 制度的核心内容。执行 DPIA 方法应当在数据处理行为开始之前进行,执行主体可以为数据控制者、数据处理者或 DPO。数据控制者负责确保 DPIA 的执行,具体执行 DPIA 可以由组织内部或外部人员完成,但数据控制者最终对该项法定义务负责。如果数据处理行为全部或者部分由数据处理者执行,则数据处理者应当协助数据控制者执行 DPIA 并提供任何必要的信息。数据控制者应当征求 DPO 的建议,DPO 应当监督 DPIA 的执行,DPO 的任命、建议和数据控制者作出的相关决定等信息应被记录在 DPIA 文档中。

(2)最低限度要求。GDPR 规定了相关组织执行 DPIA 方法的最低限度要求:系统性描述预期的处理行为和处理目的,以及对控制者所追求正当利益;对与处理目的相关的处理行为的必要性和适当性评估;对数据主体权利和自由的风险性评估;预期的风险防范措施主要包括考虑数据主体和其他相关人员的权利和合法利益,确保个人数据安全,证明符合 GDPR 要求的保障措施、安全手段和机制,而在下一次的 DPIA 方法中这些将作为已预期的风险防范措施予以考虑;为了实现 DPIA 的预期效果,有必要全面记录风险评估结果,制作标准报告,并由数据控制者决定是否将其全部或者部分公开(应当至少公开结论部分),表明数据处理活动的透明性和可问责性,以便于监管机构、企业和公众进行评估和比较;在记录存档之后,GDPR 要求控制者对数据处理行为进行监督审查(至少在处理行为导致的风险发生改变时),以评估和确认处理行为是否按照 DPIA 的评估结果进行(见图 2)。

(3)内容的可扩展性。在最低限度要求之上,

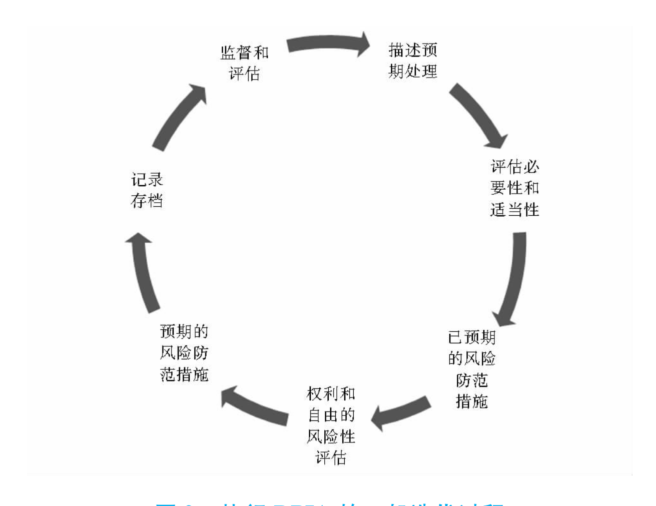


图2　执行 DPIA 的一般迭代过程

DPIA 方法的内容是可扩展的。不同的数据控制者可以灵活地确定 DPIA 的具体流程,以便与其业务实践相适应,即使是小微数据控制者也可以设计和实现适合其执行的 DPIA 方法。但是无论形式如何,DPIA 必须体现出对真实风险的评估,并允许数据控制者或者数据处理者采取措施解决这些问题。欧盟 WP29 工作组鼓励社会共同开发特定行业或者领域内的 DPIA 标准框架,使得 DPIA 可以适用于不同类型的数据处理行为以解决差异化问题。此外,DPIA 框架也应当考虑与行为准则或者行业标准的衔接问题,如果数据控制者的处理行为符合行为准则或者行业标准的相关要求,可用于证明该处理行为已经实施了适当的风险管理措施,即可免于重复执行类似的 DPIA 方法。

(4)动态调整要求。由于风险环境的快速变化,数据控制者在数据处理活动的整个生命周期持续地执行 DPIA 方法,对于在动态风险环境中保持稳定的数据保护水平至关重要。具体而言,数据控制者需要分析由处理行为的性质、范围、背景、目的的变化产生的新风险,对 DPIA 进行相应的更新。数据处理行为可能会在已经执行了 DPIA 方法并在当时达到了较低风险标准的情形下,由于风险环境的变化对自然人的权利和自由再次造成潜在的高风险,此时相关组织需要至少根据最低限度要求对 DPIA 方法进行迭代。例如某个自动化决策系统随着技术的提升变得具有社会风险性,因而触发了 DPIA 方法的执行条件;相反,某个自动化决策系统增加了人为控制因素,或者监控活动不再是系统性的,其风险评估可以表明风险水平的降低,而不再需要执行 DPIA 方法。新的数据处理技术的出现或升级将不断产生新类型的风险,作为良好实践,数据控制者应不断进行数据保护影响评估并定期进行重新评估,做到风险管理措施与风险环境的动态性相一致。

4　欧盟 DPIA 制度对我国立法的启示

4.1　欧盟 DPIA 制度下的新型数据保护模式

网络安全形势瞬息万变,“关注安全底线的、静态的、整齐划一的规定”实际上已无法为个人数据提供实质性的安全保障[23]。相对安全观显示,将风险降低到零是不切实际的,因此数据保护的主要任务是识别风险并将特定数据处理行为的风险等级降至数据控制者能够承担的水平[24]。GDPR 通过“风险路径”设定了数据控制者的一般义务,强调从数据处理行为的性质、范围、背景、目的以及对自然人的权利和自由带来损害的可能性与严重性出发,构造不同的风险治理规则,并要求数据控制者将其纳入内部决策之中,从自上而下的政府监管模式转变为自内而外的自我执行模式,这种内生的数据保护模式在降低制度执行成本的同时,有效提升了数据的保护效率和保护效果。

欧盟 DPIA 制度所构建的以风险管理为路径的新型数据保护模式,可被理解为风险评估和风险管理两个具体环节。风险评估手段可利用事实和推定评估数据处理行为对数据主体造成潜在危害的可能性,根据数据处理行为的情形与列举的潜在危害因素进行匹配,将匹配程度作为考量因素之一进行风险评估,评估结果可分为轻微、较小、一般、较高、严重 5 个等级[25]。在完成风险评估后,数据控制者需要对已经识别出的潜在危害进行风险管理。风险管理应体现在数据控制者的决策过程中,结合技术能力和社会背景,针对短期和长期的数据保护风险选择适当的防范措施。数据风险管理需要根据风险评估结果的不同等级设计不同的数据控制者保护义务:在一般风险及更低的情况下,可以适当降低或部分免除数据控制者的义务;而在较高风险和严重风险的情况下,数据控制者有更高的数据保护义务,并且有义务降低到一般风险以下。若数据控制者不能将风险控制至一般风险以下,或者难以识别或者难以评估其风险等级,则不得进行相应的数据处理行为,同时应当向监管机构进行咨询并寻求相关建议。需要指出的是,即使处在较低的风险等级下,数据控制者也应做到最低限度的保护义务,以确保数据主体的权利和自由在任何风险环境下都得到保障。

数据处理技术的快速发展和普遍应用,使得传统的监管模式难以应对大数据时代下复杂多变的数据保护问题。欧盟 DPIA 制度所提倡的数据保护模式替代了传统规制路径中“全有全无”的判断,利用风险等级

的量化，既可以提升数据保护的可操作性，也可以减少企业的合规压力，并促进数据的合理使用[26]。因此，我国的数据保护模式也应当尝试从静态的“知情同意”的传统框架转变到动态的“风险路径”思路上来，建立新型数据安全形态下的个人信息保护立法模式。

4.2 我国个人信息保护法应确立 DPIA 制度

目前，我国数据保护立法散见于网络安全法、电子商务法、消费者权益保护法、刑法修正案（七）、刑法修正案（九）以及《全国人民代表大会常务委员会关于加强网络信息保护的决定》等法律中。上述立法基本上是从数据收集和利用应遵循的合法、正当和必要原则以及数据控制者的保密、泄露通报等安全保障义务对数据控制者提出的基本要求，而对于数据保护影响评估制度并未提及。2018 年 6 月 11 日发布的国家标准《信息安全技术个人信息安全影响评估指南（征求意见稿）》（未正式通过）为机构、企业提供了个人信息安全影响评估的基本框架、方法和流程，供其自评估使用，同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供了指导和依据[27]。该标准定位于推荐性标准而非强制性标准，无强制则无保障，监管机构和问责机制的缺失将直接影响数据主体的权利救济，进而纵容企业选择性或非实质性地采用 DPIA 制度的方法以赢得市场信任，采用这一非强制性的数据保护模式甚至可能加剧自然人权益的高风险[28]。

随着信息技术的不断发展，我国的个人数据安全将面临更大的风险。欧盟数据保护框架下 DPIA 制度具备强大的事先预防能力，能够将个人和社会的数据保护风险降至足够低的水平；同时具有较强的动态性和可扩展性，能够被广泛的组织机构所采纳。我国现有立法中的环境保护影响评估和食品安全风险评估是与 DPIA 制度相类似的风险防范机制，从前者的实施效果来看，中国的立法将 DPIA 制度设置为一项强制性义务，在技术上完全可行。

通过 DPIA 义务的实施，一方面强化数据控制者的责任，使其注重在数据处理行为的全过程中增强数据保护意识和机制建设，从而赢得市场信誉和数据主体信赖。另一方面，能够实现大数据时代背景下安全和效率的平衡，治理目前普遍存在的数据滥用行为，明确要求企业组织在利用数据开展业务的同时，兼顾数据保护的安全底线，将 DPIA 义务作为其前期投入和日常运营的重要构成，在保障个人权利和自由、社会公共安全的同时，降低企业因潜在的数据危害事件带来的风险成本。因此，我国个人信息保护法有必要确定数据控制者的 DPIA 义务。

4.3 我国 DPIA 制度的构想

4.3.1 DPIA 的规制对象

DPIA 的规范对象不仅包括单一的数据处理行为，也涉及一组类似的高风险数据处理行为。判断是否为类似的处理行为，需要考虑处理行为的性质、范围、背景、目的以及风险程度是否一致，主要包括：处理行为本身是否类似、数据主体是否类似、处理行为所依托的产品或环境是否类似等因素。通常，将一组类似的数据处理行为作为 DPIA 的规制对象往往是更合理和经济的，例如公共机构计划建立数据共享的处理平台，或者多个控制者计划在某一行业内引入数据共享的应用程序，以及其他被多个主体共同使用的数据处理项目。

建立 DPIA 制度的目的在于系统性地研判可能导致自然人权利和自由的高风险的新情形。而对于已经研判过的案例——即在特定环境和特定目的下进行的相同处理行为，没有必要再进行新的 DPIA。这包括使用类似技术为相同目的收集相同类型数据的情况，以及可以适用于多个控制者的类似数据处理行为。在这些情况下，监管机构应当组织制定同一类型数据处理行为的 DPIA 标准方案并将其公开，类似行为的数据控制者应当实施标准方案中所描述的措施。如果需要使用独立的 DPIA 方案，需要向主管部门提供正当理由。而当数据处理行为涉及多个控制者时，他们需要在 DPIA 中清晰地划分各自的义务，分别负责不同的降低风险或保护数据主体的权利和自由的措施。

此外，DPIA 还可用于评估数据处理技术、产品或服务的数据保护风险，相同的技术、产品或服务可能被不同的数据控制者用于进行不同类型的数据处理行为。部署相关产品的数据控制者有义务在进行具体数据处理时执行 DPIA，但也可以选择使用由产品供应商提供的能够适用相应数据处理行为的 DPIA 方案。

4.3.2 DPIA 的适用情形

并非所有数据处理行为都需要执行 DPIA，只有在处理行为可能给自然人的权利和自由带来高风险的情况下才必须执行 DPIA。如果数据控制者不清楚是否需要执行 DPIA，特别是在引入新的数据处理技术或解决方案时，建议数据控制者执行 DPIA。因为 DPIA 是帮助数据控制者遵守数据保护法律的合规工具。对于是否执行 DPIA 的判断，数据控制者应考虑以下几种数据安全风险行为：

（1）对数据主体进行评估或评价。包括分析和预

测，尤其是使用关于数据主体的工作表现、经济状况、健康、个人偏好或兴趣，以及行为、位置、运动等方面的数据。

（2）具有法律效力或者类似重大影响的自动化决策。此类数据处理行为可能会导致特定主体对个人的排斥或者歧视。

（3）系统性监控。用于观察、监测或控制数据主体的行为，主要包括通过网络系统化收集个人数据或者对公共区域的系统化监测。

（4）处理敏感数据。敏感数据是指一旦泄露或滥用，则极易危及人身、财产安全或导致人格尊严受到损害、歧视性待遇的数据，包括身份证号码、通信内容、住宿信息、通信记录等[29]。处理敏感数据包括收集、存储、分析、对外提供、共享敏感数据的行为。

（5）大规模处理数据。在确定数据处理行为是否为大规模时，应当考虑以下因素：数据主体的数量，包括具体人数或者人口比例；数据量和数据类型；数据处理行为的持续时间；数据处理行为的地域范围。

（6）匹配或者组合数据集。对出于不同收集目的或归属于不同数据控制者的两个及以上的数据集进行关联或者合并处理的行为，这种数据处理方式将超过数据主体在一般数据处理行为上的合理预期。

（7）处理弱势群体数据。由于数据主体和数据控制者之间实力不对等的程度增加，在处理此类数据时，某些数据主体可能无法有效拒绝或者反对与其相关的数据处理行为，此时需要进行 DPIA 以降低数据主体的风险。弱势群体可能包括儿童、雇员、患者和其他需要特殊保护的弱势群体，以及数据主体和数据控制者之间存在实力悬殊的其他情形。

（8）创新性应用或者新技术的使用。新技术的使用通常可能会触发 DPIA 的执行条件，这是因为使用新技术通常意味着新形式的数据收集和使用，由此可能对个人的权利和自由带来高风险。新技术的应用将给个人和社会带来未知的后果，DPIA 制度将帮助数据控制者理解并处理此类风险。

（9）阻止数据主体行使权利、使用服务或者订立合同。这包括机构通过数据处理活动作出的自动化决策行为，例如银行通过征信数据自动化地筛选客户以决定是否向他们提供贷款。

数据控制者可通过将预期的数据处理行为与上述的风险情形进行匹配，将匹配程度作为风险因素对数据保护风险进行评估。大多数情况下，如果数据控制者认为其数据处理行为满足以上两个情形就需要执行 DPIA，除非数据控制者有充分的理由和证据表明该行为不可能带来高风险，此时数据控制者应对不执行 DPIA 的决定予以说明，并记录不执行 DPIA 的原因和主管部门的意见。

4.3.3 数据风险评估模型

数据保护评估模型是一种确保有效遵守数据保护义务的方法，该模型可以通过执行 DPIA 对特定的数据处理行为进行风险管理，协助数据控制者选择适当的预期风险防范措施以降低风险水平。数据最小化原则是数据保护评估模型的必要性原则，该原则要求任何处理行为无论是整体还是各个步骤均不得收集、处理和使用超过实现处理目的所必需的个人数据。数据最小化原则作为数据保护友好型设计的重要因素，应当嵌入至网络服务提供者的技术设计及其配置环境之中，并应用于实际的数据处理活动，贯穿数据的完整生命周期。数据保护评估模型可用于评估可能给自然人带来的权利和自由的风险，确定潜在的风险来源及损害后果。根据这些因素，DPIA 可将数据保护风险进行等级划分，以区分不同的影响程度从而确保履行相应的数据保护义务[30]。

（1）可用性。被处理的个人数据必须是可用的，并且在预期的处理活动之中能够被正确使用。数据主体必须能够有效访问数据，其数据格式应当是可识别的，数据控制者应当保证数据是按照预期的方式进行处理的。因此，数据可用性包括系统查找特定数据的能力、系统使得数据主体能够访问数据的能力以及有效展示数据内容的能力。

（2）完整性。被处理的个人数据必须要确保完好、完整和最新。数据控制者应当具备识别或者排除数据偏差的能力，以便定位或者纠正数据的属性或者内容错误。

（3）保密性。未经授权，任何人不得访问被处理的个人数据。这里的“任何人”包括数据控制者之外未经授权的第三方、技术服务提供商的员工以及数据控制者内部与相应处理行为无关的人员。

（4）不可关联性。数据处理行为应当仅被用于数据收集时的预期目的。在某些情形下，被处理的个人数据可能将被进一步地使用在预期目的之外，并与其他公开可用的数据集进行匹配或组合。这些处理行为通常超出了合理的处理目的，其仅仅在规定的特定情形下才是合法的（例如，出于公共利益的目的、出于科学或历史研究的目的、出于统计的目的，且不得侵害数据主体的权利和自由）。不可关联性通常需要通过技

术和解决方案来实现,可以利用数据匿名化等手段将后续处理与先前处理进行隔离,以确保在组织机构和信息系统内被处理的数据不存在相互关联。

(5)透明性。作为执行 DPIA 的先决条件,在数据的生成到销毁的整个生命周期内都需要具备足够的透明性。只有满足了透明性,数据主体才能在必要时表示符合法律要求的知情同意。在数据处理活动中,数据控制者需要确保数据主体和监管机构有能力识别风险并提出异议,数据主体和监管机构必须充分理解数据处理行为的相关信息:收集和处理的数据属性、为实现预期处理目的使用的信息系统和配置环境、在数据处理行为中对数据和系统安全负有安全保障义务的主体等。

(6)可干预性。数据主体在任何时候都应被有效地赋予访问、更正、删除和反对的权利,并且数据控制者有义务实施相应的权利保障措施。为此,控制者必须具备在数据处理活动的整个生命周期中干预数据属性、内容和状态的能力。

4.3.4 事先咨询义务

事先咨询义务出现在 DPIA 执行后但剩余风险仍然很高时。高剩余风险是指数据主体可能会遇到无法解决的重大的或者不可逆转的后果(例如,非法访问数据将导致数据主体遭受生命威胁、裁员、财产危险),以及当风险显而易见时(例如未能修复众所周知的漏洞)。只要数据控制者找不到足够的措施将风险降低到可接受的水平,就需要咨询监管机构。

当数据控制者所存储的个人数据已经使用适当的技术和解决方案(例如,有效的全盘加密、强大的密钥管理、适当的访问控制、完整的安全备份),并能够充分地保障数据主体的相关权利,若数据控制者认定数据保护风险已经充分降低,则可以不向监管机构咨询而开始进行数据处理活动。如果数据控制者无法充分解决已识别的风险(即剩余风险仍然很高),则数据控制者必须事先咨询监管机构。数据控制者出于公共利益目的进行的数据处理行为,也应当事先向监管机构咨询并获得事先授权。需要指出的是,无论是否需要向监督机构进行事先咨询,保留 DPIA 的记录和适当更新 DPIA 的义务仍然存在。数据控制者向监管机构进行事先咨询时应当提供以下信息:数据处理行为中控制者、联合控制者和处理者各自的职责;预期处理数据的目的和手段;保护数据主体权利和自由的措施;数据保护官的联系信息;数据保护影响评估结果等。

5 结语

DPIA 制度对组织机构应对数据保护风险起到了至关重要的作用。随着 GDPR 实施的不断深入,欧盟乃至全球范围内数据控制者将可能受到 DPIA 义务的规制。DPIA 所倡导的以风险管理为路径的数据保护模式,不仅致力于保障数据主体的权利和自由,同样能够协助组织机构合法地进行数据处理活动,降低数据处理行为带来的风险和危害。目前,我国已经启动个人信息保护立法,借鉴欧盟在数据保护立法中的先进经验,特别是探索和引入数据保护影响评估的相关制度,能够更好地应对大数据和人工智能等先进技术背景下愈加复杂多变的数据安全风险环境。

参考文献:

[1] The EU general data protection regulation is the most important change in data privacy regulation in 20 years[EB/OL]. [2019-04-23]. https://eugdpr.org/.

[2] Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679[EB/OL]. [2019-04-04]. https://ec.europa.eu/newsroom/article29/item-detail.cfm? item_id=611236.

[3] GELLERT R. Understanding the notion of risk in the general data protection regulation[J]. Computer law & security review, 2018, 34(2):279-288.

[4] BIEKER F, FRIEDEWALD M, HANSEN M, et al. A process for data protection impact assessment under the European general data protection regulation[C]//APF 2016. Lecture notes in computer science. Cham: Springer, 2016:21-37.

[5] 高富平. 个人数据保护和利用国际规则:源流和趋势[M]. 北京:法律出版社,2016.

[6] European Commission. Privacy and data protection impact assessment framework for RFID applications[EB/OL]. [2019-01-12]. https://danskprivacynet.files.wordpress.com/2008/06/infso-2011-00068.pdf.

[7] European Commission. Recommendation of 10 October 2014 on the data protection impact assessment template for smart grid and smart metering systems[EB/OL]. [2019-01-13]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:32014H0724&from=EN.

[8] VAN D N, GELLERT R, ROMMETVEIT K. A risk to a right? beyond data protection risk assessments[J]. Computer law & security review, 2016, 32(2):286-306.

[9] CLARKE R. Privacy impact assessment: its origins and development[J]. Computer law & security review, 2009, 25(2):123-135.

[10] WRIGHT D, DE H P. Privacy impact assessment[M]. Dordrecht:

Springer Netherlands, 2012.
[11] CNIL. Privacy risk assessment: methodology (how to carry out a PIA) [EB/OL]. [2019 – 02 – 01]. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf.
[12] 肖冬梅，谭礼格. 欧盟数据保护影响评估制度及其启示[J]. 中国图书馆学报，2018，44(5)：76 – 86.
[13] WRIGHT D. The state of the art in privacy impact assessment[J]. Computer law & security review, 2012, 28(1): 54 – 61.
[14] WRIGHT D, GELLERT G, GUTWIRTH S, et al. Precaution and privacy impact assessment as modes towards risk governance[M]. Luxembourg: European Commission, 2011.
[15] BERNSTEIN P L. Against the Gods-the remarkable story of risk [M]. New York: John Wiley & Sons, 1996.
[16] EWALD F. Insurance and risk[M]. Chicago: The University of Chicago Press, 1991.
[17] WYNNE B. Risk and environment as legitimatory discourses of technology: reflexivity inside-out[J]. Current sociology, 2002, 50(3): 459 – 477.
[18] POWER M. Organized uncertainty: designing a world of risk management[M]. Oxford: Oxford University Press, 2007.
[19] ISO. Risk management - Principles and guidelines [EB/OL]. [2019 – 02 – 17]. https://www.iso.org/standard/43170.html.
[20] WARNER F. Risk: analysis, perception and management - a report of a royal[M]. London: The Royal Society, 1992.
[21] 程莹. 风险管理模式下的数据保护影响评估制度[J]. 网络与信息安全学报，2018，4(8)：63 – 70.
[22] Statement on the role of a risk based approach in data protection legal frameworks[EB/OL]. [2019 – 03 – 25]. https://ec.europa.eu/justice/article - 29/documentation/opinion - recommendation/files/2014/wp218_en.pdf.
[23] 洪延青. “以管理为基础的规制”——对网络运营者安全保护义务的重构[J]. 环球法律评论，2016，38(4)：20 – 40.
[24] GELLERT R. Data protection: a risk regulation? between the risk management of everything and the precautionary alternative[J]. International data privacy law, 2015, 5(1): 3 – 19.
[25] PDPC. Guide to data protection impact assessment [EB/OL]. [2019 – 04 – 14]. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-dpias--011117.pdf.
[26] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论，2016，38(5)：92 – 115.
[27] 中国国家标准化管理委员会.《信息安全技术 个人信息安全影响评估指南》(征求意见稿) [EB/OL]. [2019 – 03 – 28]. https://www.tc260.org.cn/front/bzzqyjDetail.html? id = 20180613180739930746&norm_id = 20180523160439&recode_id = 29212.
[28] BINNS R. Data protection impact assessments: a meta-regulatory approach[J]. International data privacy law, 2017, 7(1): 22 – 35.
[29] 胡文涛. 我国个人敏感信息界定之构想[J]. 中国法学，2018，35(5)：235 – 254.
[30] BIEKER F, MARTIN N, FRIEDEWALD M, et al. Data protection impact assessment: a hands-on tour of the GDPR's most practical tool[C]//IFIP. Advances in information and communication technology. Cham: Spring, 2018: 207 – 220.

作者贡献说明：
崔聪聪：负责论文选题、大纲拟定、论文修改；
许智鑫：负责资料收集与论文初稿撰写。

Data Protection Impact Assessment: EU Legislation and China Plan

Cui Congcong　Xu Zhixin
Institute of Internet Governance and Law, Beijing University of Posts and Telecommunications, Beijing 100876

Abstract: [**Purpose/significance**] The Data Protection Impact Assessment (DPIA) introduced by the General Data Protection Regulations (GDPR) imposes new requirements on data controllers. By analyzing the relevant provisions of DPIA in GDPR and studying its legislative ideas and core concept, it could provide reference for relevant legislative work in China. [**Method/process**] This paper reviews the legal documents in the field of data protection in the EU represented by GDPR, summarizes the background and evolution of the DPIA system, and then deeply analyzes its data protection pattern, applicable situations, basic processes and execution processes. [**Result/conclusion**] The DPIA can cope with the increasingly complex and variable risk environment of data security, which has important practical value and reference significance. China's personal information protection law should establish the DPIA system, which includes DPIA's regulatory objects, applicable situations, data controllers' prior consulting obligations, and data risk assessment model.

Keywords: DPIA　risk-based approach　data risk assessment model　personal information protection law